New Amendments to the Specification:

Replace the paragraph beginning at col. 6, line 24 with the following:

The results of each sub-task, M_1, M_2, and M_3 can be combined to produce the plaintext, M, by a number of techniques. However, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme. Generally, the plaintext M is obtained from the combination of the individual sub-tasks by the following relationship:

$$\underline{Y_i \equiv Y_{i-1} + ((M_1 - Y_{i-1})(w_i^{-1} (\bmod p_i))(\bmod p_i)) \cdot w_i (\bmod n)}$$

$$[Y_i = Y_{i-1} + [(M_1 - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n]$$

where [i ≥ 2] $\underline{2 \le i \le k}$ where k is the number of prime factors of n, and

$$M = Y_k, Y_1 = C_1 \text{ and } w_i = \prod_{j<i} p_j$$

Encryption is performed in much the same manner as that used to obtain the plaintext M, provided (as noted above) the factors of n are available. Thus, the relationship

$$[C = M^e (\bmod n)] \ \underline{C \equiv M^e (\bmod n)},$$

can be broken down into the three sub-tasks,

$$[C_1 = M_1^{e_1} \bmod p_1] \ \underline{C_1 \equiv M_1^{e_1} (\bmod p_1)},$$

$$[C_2 = M_2^{e_2} \bmod p_2] \ \underline{C_2 \equiv M_2^{e_2} (\bmod p_2) \text{ and}}$$

$$[C_3 = M_3^{e_3} \bmod p_3] \ \underline{C_3 \equiv M_3^{e_3} (\bmod p_3)}.$$

where

$[M_1 = M\,(\bmod\, p_1)]$ $\underline{M_1 \equiv M\,(\bmod\, p_1)}$,

$[M_2 = M\,(\bmod\, p_2)]$ $\underline{M_2 \equiv M\,(\bmod\, p_2)}$,

$[M_3 = M\,(\bmod\, p_3)]$ $\underline{M_3 \equiv M\,(\bmod\, p_3)}$,

$[e_1 = e \bmod (p_1 - 1)]$ $\underline{e_1 \equiv e\,(\bmod (p_1 - 1))}$,

$[e_2 = e \bmod (p_2 - 1)]$ $\underline{e_2 \equiv e\,(\bmod (p_2 - 1))}$, and

$[e_3 = e \bmod (p_3 - 1)]$ $\underline{e_3 \equiv e\,(\bmod (p_3 - 1))}$.